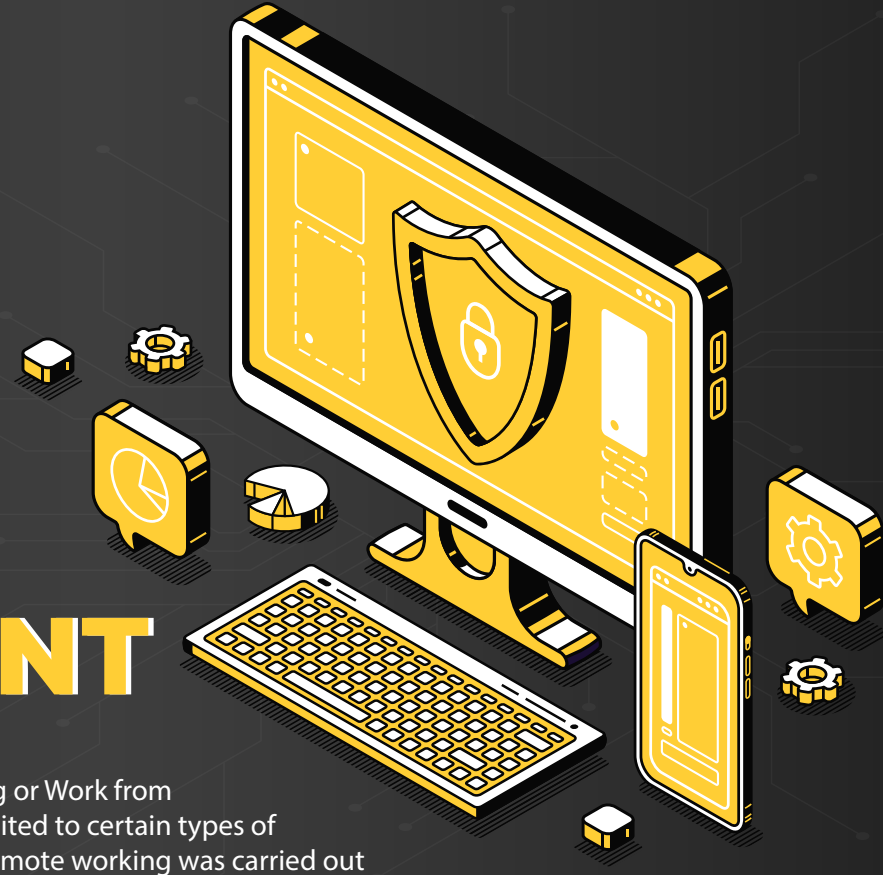
BLOCK ARMOUR

REMOTE ACCESS SECURITY ASSESSMENT



In today's hybrid work environment, remote working or Work from Home (WfH) is no longer an exception and is not limited to certain types of roles within an organization. However, the shift to remote working was carried out in an accelerated mode at the start of the Covid-19 pandemic, oftentimes without taking into account all aspects of securing remote access.

Traditional remote access tools are deployed using IPsec, SSL and TLS based gateways that tunnel traffic in from the endpoints into the corporate network. These technologies have vulnerabilities which create a conduit for malware and ransomware attacks. This is evident from recent examples of the Colonial Pipeline hack and Maze Ransomware attacks. Moreover, these legacy tools use an IP-based tunneling approach for remote access, which may pose a serious risk to an organization's security posture.

As organizations adopt a hybrid work environment, security posture assessment from a holistic perspective becomes a critical need for building effective defenses.

Block Armour offers a comprehensive remote access security assessment which provides a view of the organization's attack surface as a result of its recent implementation of remote access solutions. Our experts analyze your current exposure, identify applicable risks, and recommend appropriate measures to mitigate them.

Key Features:

The Remote Access Security Assessment attempts to identify and document:

- The various technologies and instances being employed by organizations to provide remote access to their users.
- Vulnerabilities and their exploits that may exist in the software / applications used to provide the remote access to critical application infrastructure through the Internet.
- Steps the organization can take to mitigate the identified security risks.
- Implementation of security solutions like MFA and Access Control put in place to ensure a secure access experience

Methodology:

The exercise comprises of objective and subjective activities that will present a holistic picture of the current remote access security posture as well as suggestions for improvement and future requirements. The assessment is automated and conducted using a customized toolkit developed by Block Armour to specifically assess remote access security.

Following are the highlights of the methodology:

- Identification of organization's assets exposed on the Internet by scanning using the Block Armour custom toolset based on NIST, SANS and Forrester's Zero Trust Framework
- A remote assessment of these assets to identify the attack surface's exposure to the Internet.
- A study of the external network perimeter set up by the organization in its Data Centre and Cloud infrastructure.
- Utilization of regular user credentials to access remote access tools deployed by the organization to assess access to applications.
- An assessment through these remote access sessions of the network connectivity to expose the risks through these connections.

Outcome:

The outcome of this exercise will offer the organization:

- A single comprehensive view of all Internet remote access gateways across the environment.
- A security posture assessment of remote access security mechanism and any associated risks exposed by them.
- Recommendations to mitigate any identified security risks.

Duration:

The duration of such assessment will be no more than 2 weeks. It will depend on the tools and technologies deployed for enabling remote work channels as well as the geographical scale.

For more information or to request an assessment, **please email us at info@blockarmour.com**

www.blockarmour.com
+91 8095818123
twitter.com/BlockArmour
www.linkedin.com/company/block-armour

BLOCK ARMOUR